Strategies for Mixed Criticality ARINC661

Limiting Airworthiness Impacts When Adding New Capabilities to Existing Systems

The Open Group FACE™ Army TIM Paper by:

Steven P. Price, Software Engineer, CMS Team/FACE TSS SC Lead

Christopher J. Edwards, Systems Engineering Lead, CMS Team

Rachel D. Moudy, Software Engineering Lead, CMS Team

May 26, 2021

Table of Contents

Executive Summary 4

Problem Space 5

Mixed Criticality and a Common Mission Computer 6

Flight Critical Systems 6

Mission Capabilities are not DAL A 6

Common Mission Computer CDS 6

Separation of Criticality 7

Separate Devices 7

Separate Processes 8

Separate Configurations 8

Techniques for Separation of CDS Configuration 10

Menu/Page Control and “Super Layer” 10

Connectors 10

Configure Overall Page List 10

Configure Menus 11

Configure Capability Options 11

Configure a PDI List 11

Single CDS or Multiple CDS 12

High Criticality using External Source for Low Criticality 12

Limited Widget Sets for High Criticality 12

How to handle Interactive Widgets 12

Menu System Support Through a Limited Widget Set 13

Map Horizontal and Map 3D 13

Conclusion 14

References 15

About the Author(s) 16

About The Open Group FACE™ Consortium 17

About The Open Group 17

Executive Summary

As future systems move to helmet displays and large format single systems to present all information to the crew, the separation of criticality will be vital in reducing the full costs of these systems.

The separation of criticality in processing information plays a significant factor in the qualification costs of avionics systems. A system presenting flight-critical information must be qualified to a higher level, leading to higher qualification costs.

Additional capabilities added to aircraft are rarely at higher qualification levels of the initial system development. The ability to add lower criticality information that can integrate with higher criticality information without modifying the existing higher criticality system reduces efforts of adding new capabilities.

ARINC-661, and the approach taken in its implementation, can greatly reduce the costs of adding capabilities to a platform.

Problem Space

One of the goals is to reduce the cost of future aircraft through the development of a common Modular Open System Approach (MOSA) across the existing platforms that will be used on future aircraft systems. Effective use of this strategy will allow existing platforms to offset costs of future platforms and move all multiple platforms to a family of systems that can effectively share new capabilities. As part of the desire to support mission capability presentation on displays that support flight-critical information, separation of criticality in the processing and configuration is integral to the MOSA.

The use of the Future Airborne Capability Environment (FACE) Technical Standard as a software architecture framework provides a foundation for rapid integration of capabilities from multiple vendors who develop to that architectural framework. This was demonstrated at multiple integration events, including the Rapid Integration Framework demonstrations in 2018 (Edwards C. J., Rapid Integration Framework (RIF) Demonstration Information Packet, 2018).

All editions of the FACE™ Technical Standard have been well justified in recommending ARINC-661 to present user interfaces within this architectural framework (Edwards & Price, Architectural Approaches in Evolution of Emerging Technologies, 2020). The utilization of ARINC 661 as a windowing system within a system architecture that is aligned to the FACE Technical Standard can assist in reducing qualification costs and allow for streamlined information from multiple, separate Units of Conformance (UoCs) on a single display.

Utilizing an Integrated Modular Avionics (IMA) approach-based qualification strategy, software systems are developed with qualification artifacts separate from the other aspects of the end system (RTCA, Inc, November 2005). The ARINC 661 Cockpit Display System (CDS) is a configurable core component that can be compiled and qualified, then configured by a set of configuration files. The CDS is a critical core component for a system supporting hosted capabilities with graphical representations (Edwards, Price, & Mooradian, The Impact of the FACE Technical Standard on Achieving the Crew Mission Station (CMS) Objectives, October, 2017).

The use of Parameter Data Items (PDI) for configuration is covered in DO-178C (RTCA, Inc, 2012). If a system is to support hosted UoCs of mixed criticality, then establishing qualification zones can save qualification efforts, as capabilities are added (Edwards C. J., Establishing Qualification Zones in a Core System, 2019). Examination of the system parameter data items (PDI) in light of qualification zones can ensure that the addition of a low criticality capability does not influence the PDI used in higher criticality artifacts.

The objective of this paper is to present the separation of processing capabilities for higher criticality functions and the separation of the configuration (PDI) of configurable core components across a mixed Design Assurance Levels (DAL) system. This can provide a path for the rapid deployment of low-criticality functions without re-qualifying the flight critical systems that will display the resulting information.

Mixed Criticality and a Common Mission Computer

Functionality in ARINC-661 is separated between a CDS and User Applications (UAs). The CDS is a configurable core system component. Hosted capabilities presenting information are implemented as UAs (AEEC - Engineering Standards for Aircraft Systems, 2019). Separation of criticality using a multi-layered CDS approach should be considered along with the use of ARINC 661 for new capabilities.

Flight Critical Systems

Enduring aircraft have their own flight-critical avionics system that would be costly to requalify if an extensive ARINC-661 CDS was added. Therefore, some enduring platforms may never migrate the primary flight display to ARINC 661. Yet, the ability to display information from an ARINC-661 implementation on the primary flight displays, Head's Up Displays (HUDs) and Helmet Mounted Displays (HMDs) are desirable.

Future systems may implement all critical flight functions following ARINC-661, enabling better flexibility for change and better separation of fight critical functions. Still, the higher qualification costs of the CDS may present a desire to have limited support for interactive widgets and touch screen interfaces for those higher criticality functions.

If an ARINC-661 solution is used in the flight critical systems, the use of the Definition Files (DF), and Connector References between criticality levels may warrant special care to ensure additional lower criticality functions do not impact the higher criticality configuration.

Mission Capabilities are not DAL A

Mission capabilities designed for a common mission computer will not have a flight catastrophic impact on the safety of the aircraft. The design of a common mission computer will not include triple redundancy and differing design requirements to support this level of criticality. It may be sensible to develop a CDS to a lower criticality level for mission functions that are not needed by the flight critical systems. This CDS can support a wider set of core capabilities to mission functions.

Having a distinct set of configuration files for the mission functions also assists in reducing the cost of bringing new mission functions to the existing aircraft systems.

Common Mission Computer CDS

A CDS deployed to a common mission computer can utilize video connections to existing display systems or other means of transferring the images to the flight critical systems.

Alternatively, a low criticality CDS supporting separation of PDI criticality can be deployed on separate displays accessible to the crew. This provides a more traditional approach to get new functions on an existing cockpit without affecting flight qualification. However, this pattern does not provide a path to full integration of low criticality functions within high criticality displays and it adds a new display to the crew scan.

Separation of Criticality

The development of separate configurations for different levels of criticality should take into account the levels of criticality that the system supports (Edwards C. J., Establishing Qualification Zones in a Core System, 2019). For most aircraft, it is easy to separate the flight critical DAL-A systems from the lower criticality mission systems. DO-178-C describes criticality into five levels. When the criticality goes up, so does the effort to qualify the system that supports it. These qualification efforts can double the system's total cost when the system supports the highest criticality functions. Aircraft functions are allocated across these five levels, and most aircraft will have functions that fall into all five levels of criticality, but it is often impractical to develop to all five levels and provide enough evidence to support the separation.

There are several ways to separate a system within zones of criticality. For the separation of graphical processing using ARINC-661, the separation can occur as two separate systems. Future systems patterned after the F-35 helmet display or a singlewide touchscreen interface should include the ability for mission functions to be integrated through a separate, low criticality system with its own configuration.

The desire for mixed criticality displays to a single presentation requires the final display to be developed at the highest criticality level. This system can be fed information from lower criticality systems that can be separated from the higher criticality display in various ways.

Proper partitioning of criticality includes the allocation of time, memory, and resources to ensure one installed capability cannot affect another. With the increase in the use of multicore processors and multi-layered memory cashes, the problems have become increasingly complex. Separation of criticality by processing card is easier to prove than separation of partitions within a single multi-core processor.

Partitioning strategies also play into a product line approach to the artifacts for software components distributed across multiple platforms. Many qualification artifacts developed for the CDS or reusable User Applications are readily transferable (designs, requirements, test cases, development artifacts, etc.) while others will be impacted by the deployment options. A strategy for maximum reuse of the technical data package (TDP) for a software package is directly impacted by having a common partitioning strategy across multiple platforms.

Separate Devices

One method of separation is to run lower criticality functions on a separate system from the higher criticality functions. In a traditional ARINC-661 view, this would be implemented as a CDS developed to the highest criticality running on a display system. The lower criticality functions would then be implemented as UAs running on a separate processor using a transport connection between the systems.

There are clear advantages to safety if each criticality level has its own processing. The only interfacing concern between a higher criticality system and a lower criticality system is when a lower criticality inputs to the higher criticality system. These inputs must either drive lower criticality functions or have additional measures factored in to satisfy the safety analysis; they can then be factored into a higher criticality function.

Suppose the higher criticality system is designed to support an evolving set of lower criticality functions (as with an ARINC 661 CDS). In that case, the configuration of the higher criticality capabilities should be separated from the processing of the lower criticality inputs. If the addition of a low-criticality function effects high-criticality configuration, the impact of the addition has a larger than necessary impact.

An alternative to the traditional ARINC-661 deployment is a mission CDS that presents information to a flight critical CDS combined into a single presentation. This pattern allows for a clear separation of configuration into separate zones on condition that the flight critical CDS configuration allows for the flexibility the lower criticality CDS may need.

Separate Processes

Partitioning within a single system can save on Size, Weight, and Power (SWaP) and make more efficient use of powerful multi-core processors. This could allow for the use of a single CDS using the EGL Compositor[1] to support high criticality functions while allowing for the addition of lower criticality functions within the same processor.

Separation of criticality within a single system can be accomplished through ARINC-653 partitioning. Analysis of partitioning and the interference patterns between processes using the same resources must be performed, which increases the qualification costs of such a system.

When those processes support differing levels of criticality, the separation of configuration between criticality levels should be considered. The qualification efforts for the more frequent integrations can be reduced if it is envisioned that lower criticality functions will be added at a greater frequency than the higher criticality functions.

The configuration of an operating system schedule is an area of particular concern. If the overall schedule is impacted when a low criticality function is added or modified, there is an impact on the higher criticality PDI (Edwards C. J., Establishing Qualification Zones in a Core System, 2019).

Separate Configurations

When one process/partition supports functions of mixed-criticality, the entire process must be tested to the highest DAL. The PDI impact on flight functions need to be tested to the highest criticality of the system. Qualification efforts of lower criticality additions/changes may potentially be reduced if there are separate configurations for the higher criticality functions than from the lower criticality functions.

Developing a single CDS that provides mixed criticality should also separate its configuration into qualification zones. This ensures that addition of low criticality functions does not influence the prior qualification of higher criticality functions.

The testing of a process that uses this sort of PDI separation will call for testing the higher criticality functions against a set of dummy lower criticality PDI and functions to prove changes to the lower criticality

[1] The EGL Compositor is defined by the Khronos® Group as part of the EGL Standard and is recommended by the FACE Technical Standard Edition 3.0 and later as a means to provide window management of OpenGL windows.

PDIs do not impact the higher criticality functions. Once established, the same tests can be executed when the higher criticality PDIs are tested.

Techniques for Separation of CDS Configuration

On a single display, including helmets and full cockpit displays, the need to provide flight-critical information as the pilots' main source of information drives the primary display of that information to the highest level. A pilot must have access to the flight-critical information when they need it, without having the possibility of lower criticality functions blocking their access.

Most CDS implementations will support the concept of a page system. A "Page" is a high-level collection of information related to each other (such as a Primary Flight Display, EICAS display, or Map). Information from capabilities is placed on these pages. Some pages will support information of mixed criticality. The ability to select a page containing high criticality information must be at the criticality of that page.

Menu/Page Control and "Super Layer"

The top-level configuration of pages is sometimes referred to as the "Super Layer." This is usually the set of widgets that are always visible and a collection of pages that are mutually exclusive (using a form of Mutex widget). This can be implemented using the specific Super Layer widgets or by using the standard ARINC-661 widget set.

Setting the mutex "visible child" controls which page is displayed. The setting of the page should be accomplished through a page controlling user application. It is recommended that this application serve as the top-level menu system and handle any user input interfaces that can be directed at the highest criticality applications (Price & Edwards, 2017).

Connectors

Windows defined in the super layer define clipped areas within a page where an individual UA can render a layer of its own. The method for tying the window to the UA layer is a connector widget. The connector widget uses an ID to identify what UA layer will be used in the window. In a mixed-criticality system, the main "super layer" will be at the highest criticality. A method for pointing to lower criticality windows should be established so that adding new lower-level pages does not change the super layer configuration. This means the definition of the connector list should follow the same PDI breakdown for mixed-criticality within the system. The connection list should be implemented as a chain of connection lists for each criticality level so that adding a lower criticality UA has no impact on PDIs used in higher criticality applications.

Configure Overall Page List

The separation of PDI based on qualification zones also affects the menu system that controls the visible page. The comprehensive list of pages can be broken down into sections for each level of criticality. The configuration of how the high criticality pages are accessed would have precedence over any lower criticality PDI. Following lower criticality page's lists can configure the access to those pages within limits available to the lower criticality PDI. This structure can be extended to any number of criticality levels.

Common Symbology Approach Using Configurable Core Symbology

Configure Menus

The configuration of individual menus in the menu system will follow the same pattern. Menus supporting the highest criticality functions will be defined in a separate PDI (or set of PDIs) that will effectively define the boundaries for the lower-level menu functions. The higher criticality menus will include a means to access high criticality functions regardless of the lower criticality configuration.

Configure Capability Options

Capabilities added to a system may be implemented as UAs or may simply be a set of states and command interfaces on the transport layer. Each capability will have a set of functions and states that might be displayed by the menu system. The configuration of options for a capability (including connections to transport) can be broken down per capability PDI files. These PDIs will define the options available for the configurable menus.

Configure a PDI List

For both the menu system and the CDS, the list of PDIs may need to be carefully planned. If all PDIs were loaded in a single list or file, then the list would need to be updated as new capabilities are added. A separate list for each qualification zone can solve this problem.

Single CDS or Multiple CDS

A single ARINC 661 CDS can be implemented to support multiple DAL levels. In order to accomplish this, all widgets used by the single CDS will need to be tested to the highest DAL. Therefore, the CDS must implement strategies for separation of DAL in its configuration, as discussed above.

Another approach is to have more than one CDS implementation. Consider a solution where high criticality (DAL A and DAL B) functions are to be mixed with functions at DAL C or DAL D. Implementation of some more complicated widgets, such as multi-touch gestures, could be implemented only in the lower criticality CDS, reducing the qualification costs and the effort of implementing CDS functions into the higher criticality systems.

High Criticality using External Source for Low Criticality

The use of an external source widget to display the contents of another CDS is an effective way to partition out CDS functions between zones of criticality. In this implementation, the higher criticality configuration includes external source definitions for areas that would be defined in the lower criticality CDS configurations. The lower criticality CDS may have multiple "super layers", one assigned to each external source.

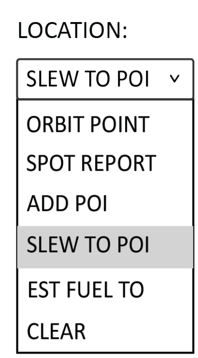
The means of getting image information to the external source is dependent on the overall system architecture. A lower criticality CDS on the same processing hardware could share graphics processing unit (GPU) and graphics memory and make use of the EGL Compositor extension.

A lower criticality CDS on another processing resource could use a streaming video service (which may introduce lag) or a video channel that uses firmware level video mixing. This means of sending video information would use an additional connection between the computers (that of a video stream) and offers advantages of lower latency and a reduction of processing resources on the higher criticality system.

Limited Widget Sets for High Criticality

Another advantage of separating CDS implementations is the cost of qualification for the CDS. A CDS supporting the minimal set of widgets has fewer lines of code, therefore fewer qualification costs, than one supporting more widgets. If a lower criticality CDS supports functions like the interactive widgets, the qualification of the gesture processing is only at the lower criticality. This will limit the graphical capabilities available to higher criticality functions but presents great cost savings to enduring systems that already have their flight-critical solutions in place.

How to handle Interactive Widgets



Interactive widgets are a set of widgets beyond the minimum set called out in the FACE Technical Standard. These include buttons, scroll lists, combo boxes, and the like. These interactive widgets could be supported by a lower criticality CDS if the means of interaction are passed to the lower criticality widget.

Example: Support of the gesture widget would include additional configuration information for the lower criticality CDS as well as access to the touch inputs of the display. The lower criticality CDS would need to configure the touch information as well as the actual location of each external source.

Menu System Support Through a Limited Widget Set

If the high criticality system supports a system-wide menu, the menu system will be limited to the basic widget set. This may lead to a separation of the menu between the high criticality system using physical interfaces and a lower criticality system using interactive widgets. This does not present a problem for capability additions across differing implementations on the aircraft platforms. The menu system for the platform will operate in a consistent manner. Additionally, it is abstracted from the capability software through the common command interface (Price & Edwards, 2017).

Map Horizontal and Map 3D

The map widgets present another unique issue when addressing mixed criticality. The display of a map, particularly a 3D map, is most efficient if the rendering is performed in a single process that is aware of the map view perspective and everything that must be rendered. A reading of ARINC 661 implies that the geo-to-pixel rendering of symbology on a map should be handled by the CDS. This places the onus geo-correlation within the CDS. In a mixed DAL environment, that leads to a complex set of code that would require additional burden on a CDS supporting higher criticality functions.

Therefore, from a functional allocation perspective, the separation of the 2D and 3D map rendering from the CDS is beneficial. It is better to implement the map functions separate from the CDS and use an external source mechanism for rendering the result into the CDS managed windows.

The communication of symbology to the Map capability can be through ARINC 661 messages forwarded to the map or symbology obtained through a key interface associated with Common Operating Picture data.

This was demonstrated at the 2018 PEO Aviation FACE TIM and Expo (Edwards C. J., Rapid Integration Framework (RIF) Demonstration Information Packet, 2018). If a separate key interface is used, it should be handled in an abstract manner so that additional types of symbols do not lead to additional types of messages. Many map implementations currently used by Department of Defense (DOD) platforms are not using the ARINC-661 interface or the FACE Transport Services Segment (TSS) interfaces. As these map products are integrated into mission systems, they should be integrated using a set of Common Operating Picture key interfaces. Therefore, support of an ARINC-661 map item list is a key interface that may be used by additional UoCs.

Conclusion

An implementation of a MOSA approach to ARINC 661 should include the development of a mission computing CDS for the display of functions in the lower criticality DAL. This CDS should be configured to send graphical data to a higher criticality system using a transfer of completed images through video transfer options depending on the platform.

A product line approach to a common CDS will provide for maximum reuse of TDP data. A strategy for reuse is built in, starting with the Plan for Software Aspects of Certification (PSAC) and continuing to every document it references. A CDS following this approach should support multiple physical display formats through configuration.

Flight critical systems implementing ARINC-661 functions should support the separation of criticality in the configuration and include strategies like configurable core graphical components (Edwards, Price, & Moudy, Common Symbology Approach Using Configurable Core User Applications (UAs), 2021).

Integration of capabilities into a system that includes both a low-criticality and a high criticality CDS will allow programs to make decisions that allow for the rapid deployment of capabilities. Thus, creating a tighter integration to the primary displays at a point that coincides with a major system update.

The use of the external source layering can allow for future additions of other common user interface approaches that are not in alignment with ARINC-661 approach recommended by the FACE Technical Standard. Therefore, an external source widget combined with some interactive widgets could be provided to an Android or Web-based interface to support low criticality functions not initially designed for aircraft use.

References

(Please note that the links below are good at the time of writing but cannot be guaranteed for the future.)

- AEEC - Engineering Standards for Aircraft Systems. (2019). *ARINC 661.*
- Christopher J. Edwards, S. P. (2021). *Common SYmbology Approach Using Configurable Core User Applications (UAs).* The Open Group.
- Edwards, C. J. (2019). *Establishing Qualification Zones in a Core System.* The Open Group.
- Edwards, C. J. (January 2016). *Developing Portable/Reusable Certification Artifacts.* The Open Group.
- Edwards, C. J., & Mooradian, D. (September, 2017). *The FACE Technical Standard Applied to a Comprehensive Architecture Strategy.* The Open Group.
- Edwards, C. J., & Price, S. P. (2020). *Architectural Approaches in Evolution of Emerging Technologies.* The Open Group.
- Edwards, C. J., Price, S. P., & Mooradian, D. H. (October, 2017). *The Impact of the FACE Technical Standard on Achieving the Crew Mission Station (CMS) Objectives.* The Open Group.
- FAA Certification Authorities Software Team. (2016). *CAST-32A Multi-core Processors.*
- FACE Consortium. (24 Jun 2014). *Technical Standard for Future Airborne Capability Environment (FACE), Edition 2.1.* The Open Group. Retrieved from www.opengroup.org/library/c145
- FACE Consortium. (December 2017). *Technical Standard for Future Airborne Capability Environment (FACE), Edition 3.0.* The Open Group. Retrieved from www.opengroup.org/library/c17c
- PEO Aviation. (2018). Rapid Integration Framework (RIF) Demonstration Information Packet. *Proceedings of the 2018 September US Army FACE™ Technical Interchange Meeting.* Huntsville, AL: The Open Group.
- Price, S. P., & Edwards, C. J. (2017). *A Common Command Interface for Interactive FACE Units of Conformance.* The Open Group.
- RTCA, Inc. (2010). *AVIONICS APPLICATION SOFTWARE, ARINC SPECIFICATION 653P1-3.*
- RTCA, Inc. (2012). *DO-178C, Software Considerations in Airborne Systems and Equipment Certification.*
- RTCA, Inc. (November 2005). *RTCA DO-297, Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations.* RTCA, Inc.

About the Author(s)

Steven P. Price has been working in avionics and embedded software for more than 30 years. He has worked on several different graphic user interfaces, including cockpit systems. He has been a leader in the design and implementation of some of these systems, along with being involved with the testing of some of these systems. Currently, Mr. Price is one of the Principal Software Engineers for RIF and the principal developer of the CMS Menu System. He is a co-lead on the FACE Transport sub-committee and FACE Verification Authority Subject Matter Expert (SME), along with involvement in other FACE sub-committees.

Christopher J. Edwards has been working in the avionics industry for over 25 years, primarily on cockpit systems for military aircraft. In those years, he has served in leadership roles in System Architecture, Software Development, Requirements Capture, PVI development, Qualification Testing, and Project Management. Mr. Edwards work within the FACE Consortium has been as a principal author on both the FACE Conformance Policy and the FACE Technical Standard as well as many other consortium documents. Mr. Edwards currently leads the FACE Conformance Overview presentations and serves as a co-lead of the FACE Technical Working Group (TWG) Conformance Verification Subcommittee and as the facilitator of the FACE Verification Authority Community of Practice. Mr. Edwards serves as a MOSA Subject Matter Expert and is the Chief Architect and Systems Engineer for the Fixed Wing Family of Systems as well as other RIF related projects.

Rachel D. Moudy has been working in the missile defense and avionics industry for the past 9 years designing, developing, and integrating military software solutions. Currently, Mrs. Moudy supports the CMS team as the Software Engineering Lead and the Systems MBSE Lead for the Fixed Wing Family of Systems. She continues to acquire knowledge of user and design interactions to improve and create innovative solutions. Mrs. Moudy is currently pursuing a Master of Science in Human Factors with a concentration in Aerospace to ensure warfighter's behavior is captured throughout designs.

About The Open Group FACE™ Consortium

The Open Group Future Airborne Capability Environment™ Consortium (the FACE™ Consortium) was formed as a government and industry partnership to define an open avionics environment for all military airborne platform types. Today, it is an aviation-focused professional group made up of industry suppliers, customers, academia, and users. The FACE Consortium provides a vendor-neutral forum for industry and government to work together to develop and consolidate the open standards, best practices, guidance documents, and business strategy necessary for the acquisition of affordable software systems that promote innovation and rapid integration of portable capabilities across global defense programs.

Further information on the FACE Consortium is available at www.opengroup.org/face.

About The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. Our diverse membership of more than 800 organizations includes customers, systems and solutions suppliers, tools vendors, integrators, academics, and consultants across multiple industries.

The mission of The Open Group is to drive the creation of Boundaryless Information Flow™ achieved by:

- Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies
- Offering a comprehensive set of services to enhance the operational efficiency of consortia
- Developing and operating the industry’s premier certification service and encouraging procurement of certified products

Further information on The Open Group is available at www.opengroup.org.